

CIBERDELITOS Y PROTECCIÓN DE DATOS PERSONALES

Antoni Bosch Pujol , CISA, CISM, CGEIT, ECPD

Director General del Institute of Audit & IT-Governance (IAITG)

Director del Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC

de la Universidad Autónoma de Madrid (MASGDTIC)

Profesor de la Pacífico Business School

Dr. Francisco Olaso Martins

Abogado; Certificado en PLAFT (CAMS); Certificado en Asesoramiento en Inversiones.

Profesor del Certificado en Prevención de Lavado de Dinero y Financiamiento del Terrorismo, UCU Business School.

Consultor en BST Global Consulting

Importancia de los datos en la era digital

***“Los datos son el nuevo oro
de la Economía Digital”***

Neelie Kroes, Vicepresidenta de la Comisión Europea y responsable de la Agenda Digital.
Enero 2012.



2005



Luca Bruno / AP

2013



NBC NEWS

Michael Sohn / AP



internet

7mo. CPLD Q FT

¿Qué hay de nuevo?

Marketing de

Redes Sociales!

Haz llegar tus mensajes a través de nuevos medios

A horizontal row of various social media icons, including Twitter, Facebook, LinkedIn, YouTube, and others, arranged in a slightly overlapping manner.

ANTES DEL SOCIAL MEDIA DESPUÉS DEL SOCIAL MEDIA



twitter

Google+

morfipec.com

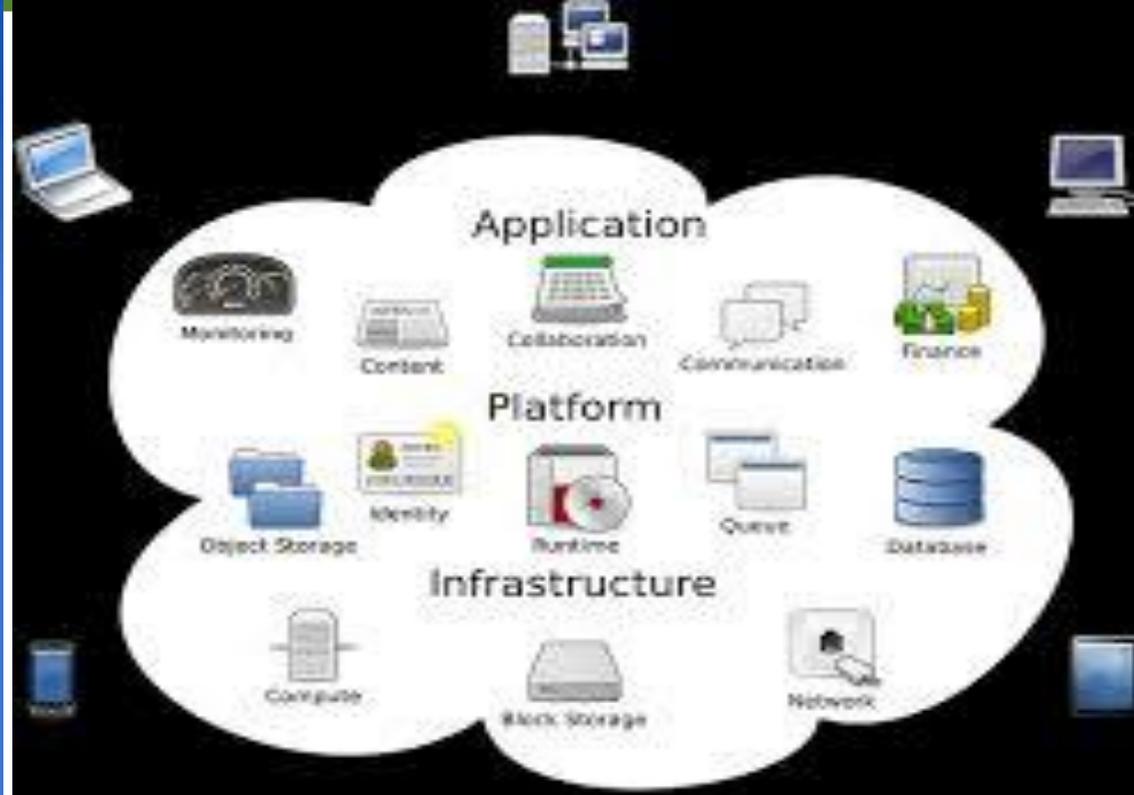


myspace

bado

Gonico







SE TRATA DE CONECTAR OBJETOS A LA RED PARA QUE SEAN CAPACES DE INTERACTUAR ENTRE ELLOS Y CON NOSOTROS

LA SUMA DE SENSORES DE MÁQUINAS, SOFTWARE, HUMANOS, LA NUBE Y EL INTERNET, QUE LLEGARÁ A SER TAN COMÚN COMO LO ES HOY EL INTERNET DE LAS PERSONAS.



VIDEO VIGILANCIA



DRONES





¿QUÉ PASA EN
1 MINUTO
EN INTERNET?



Fuente: Exelacom Inc.

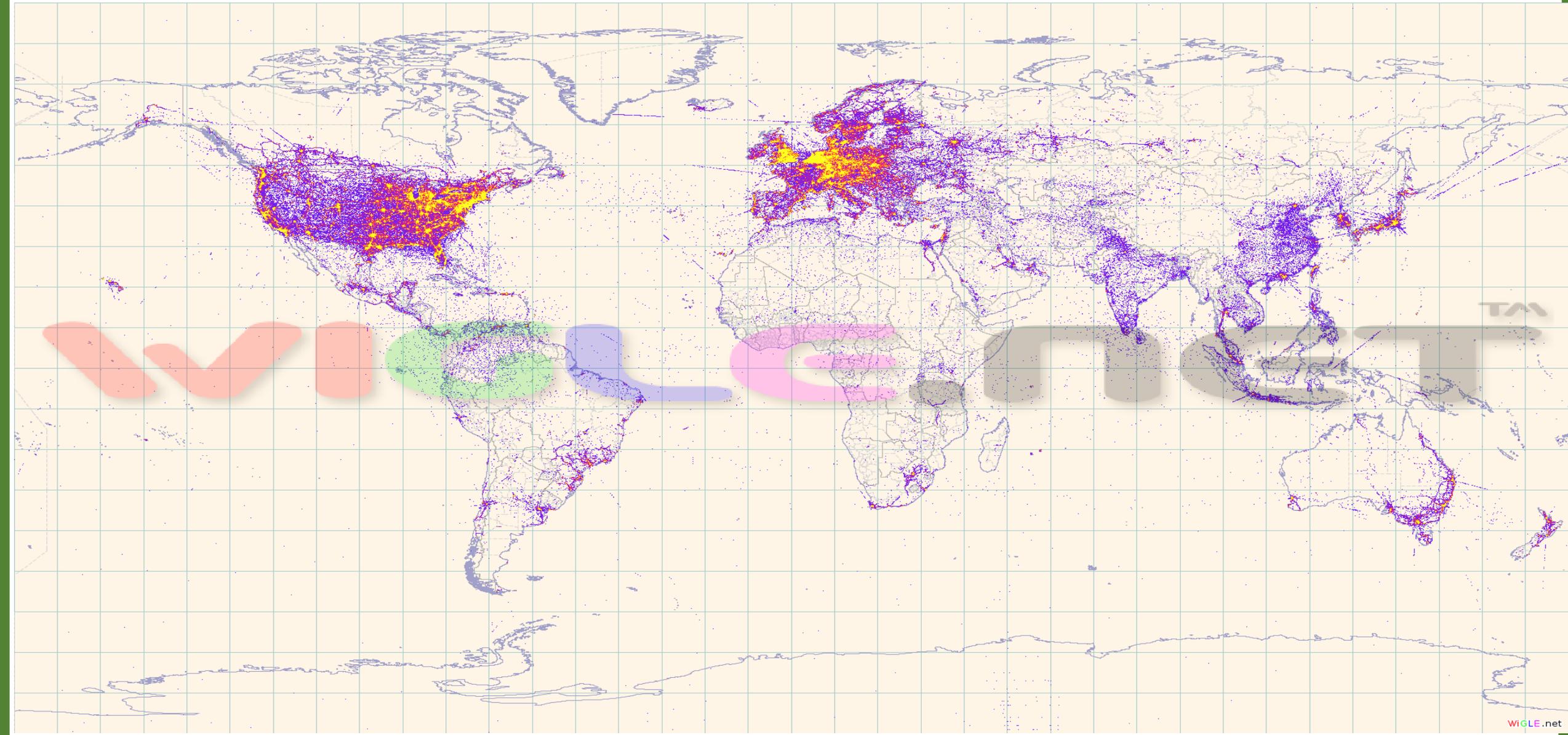
Expansión

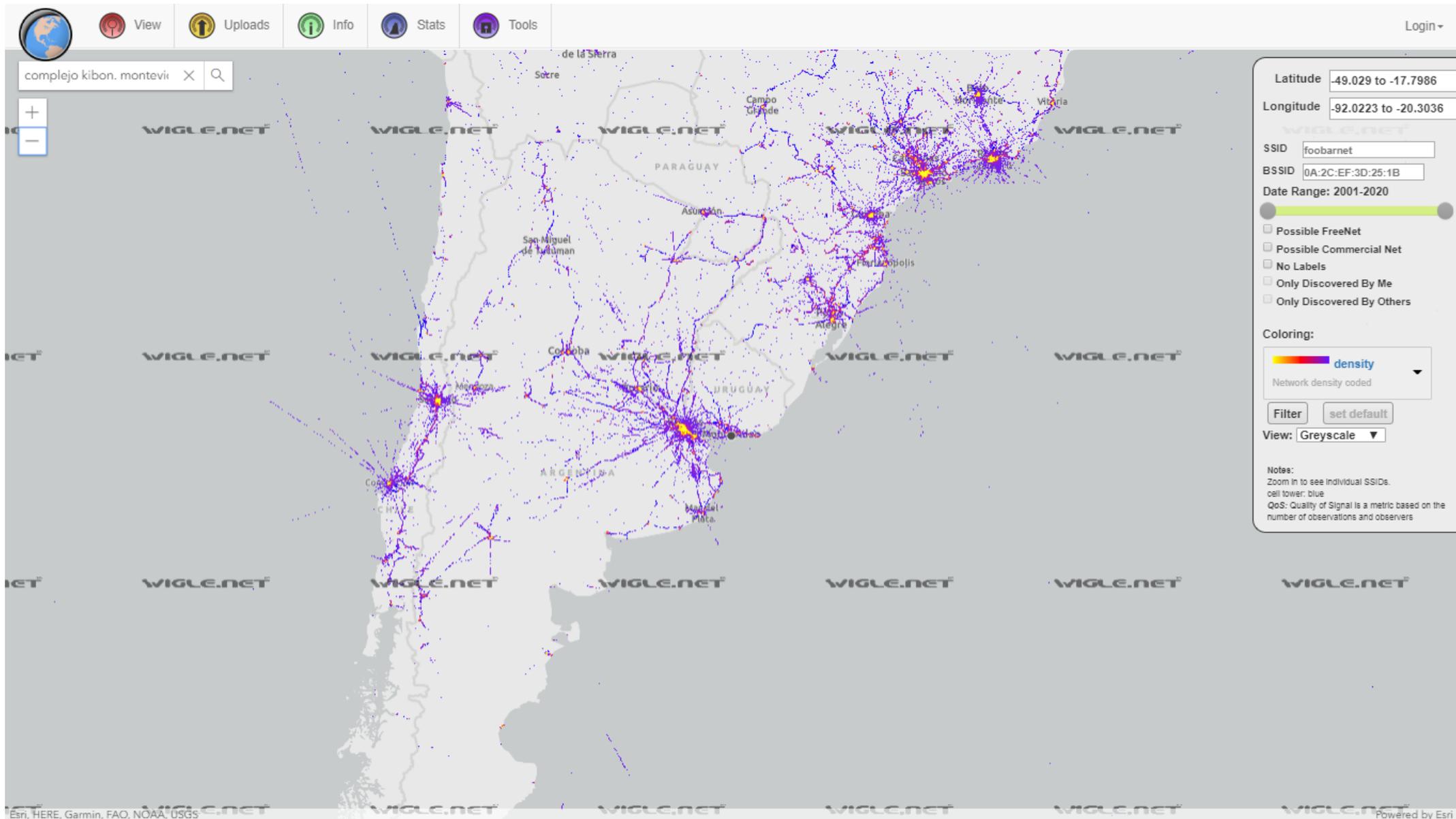


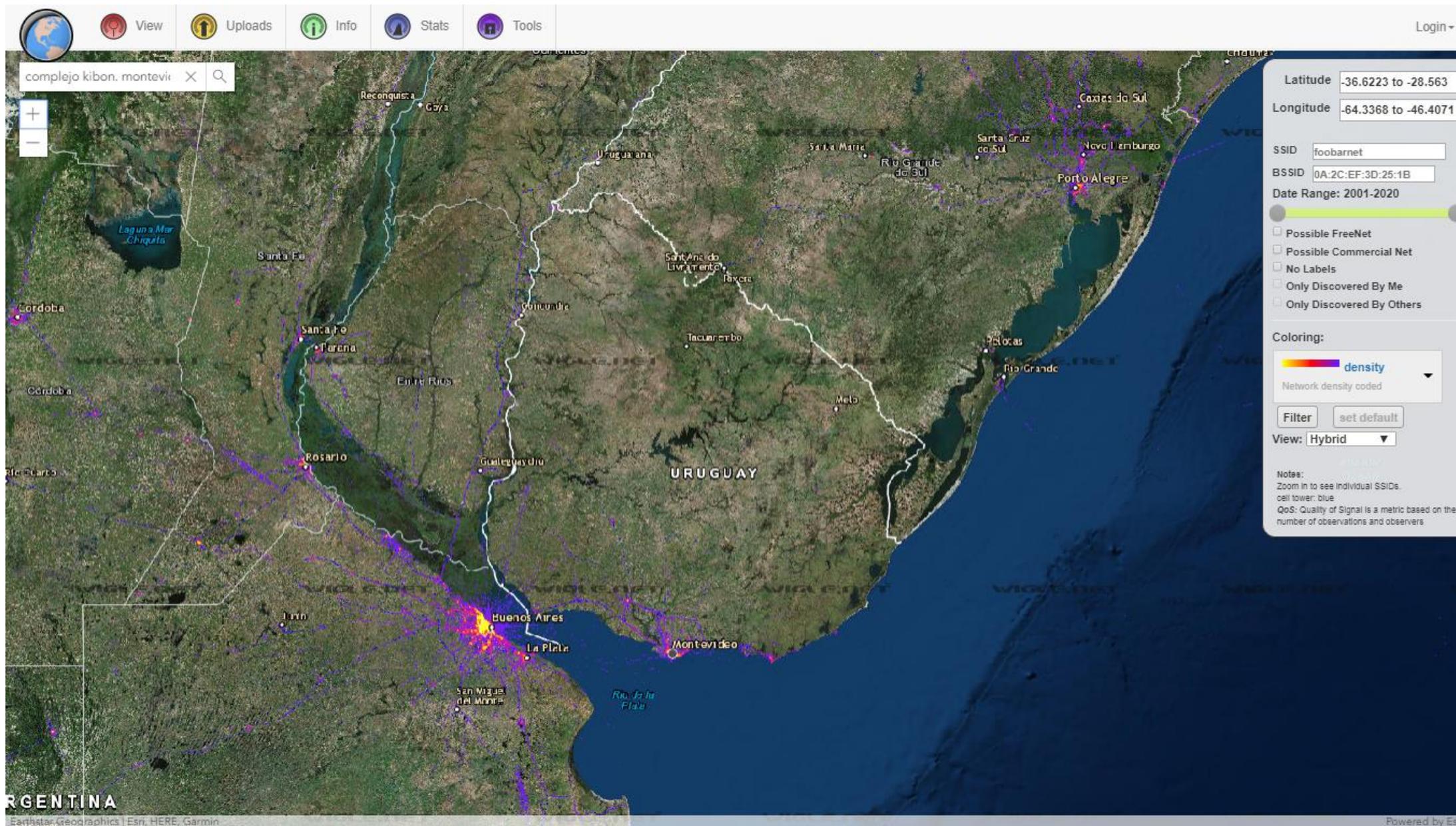
CONTROL DE RIESGOS



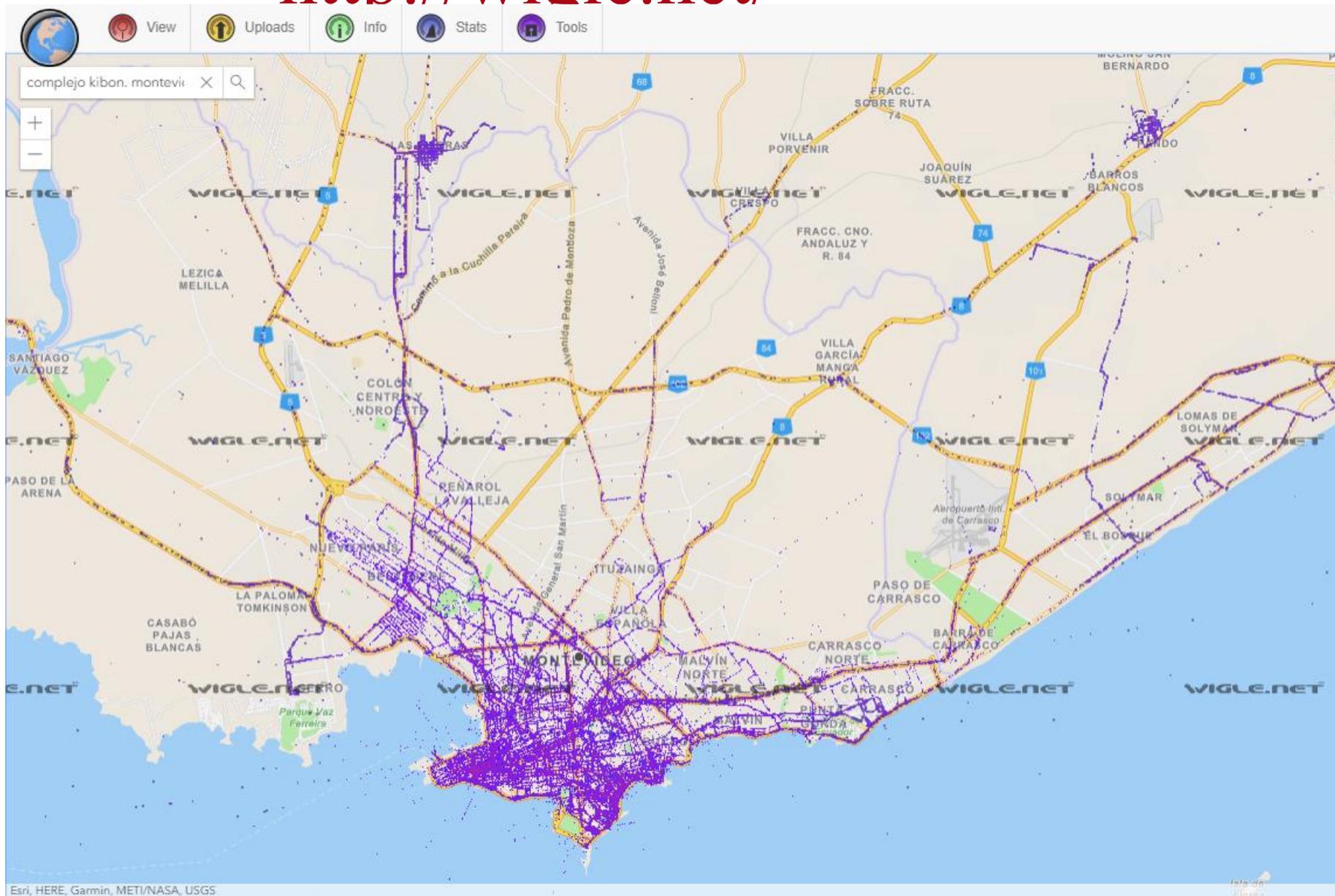
<http://wicle.net/>



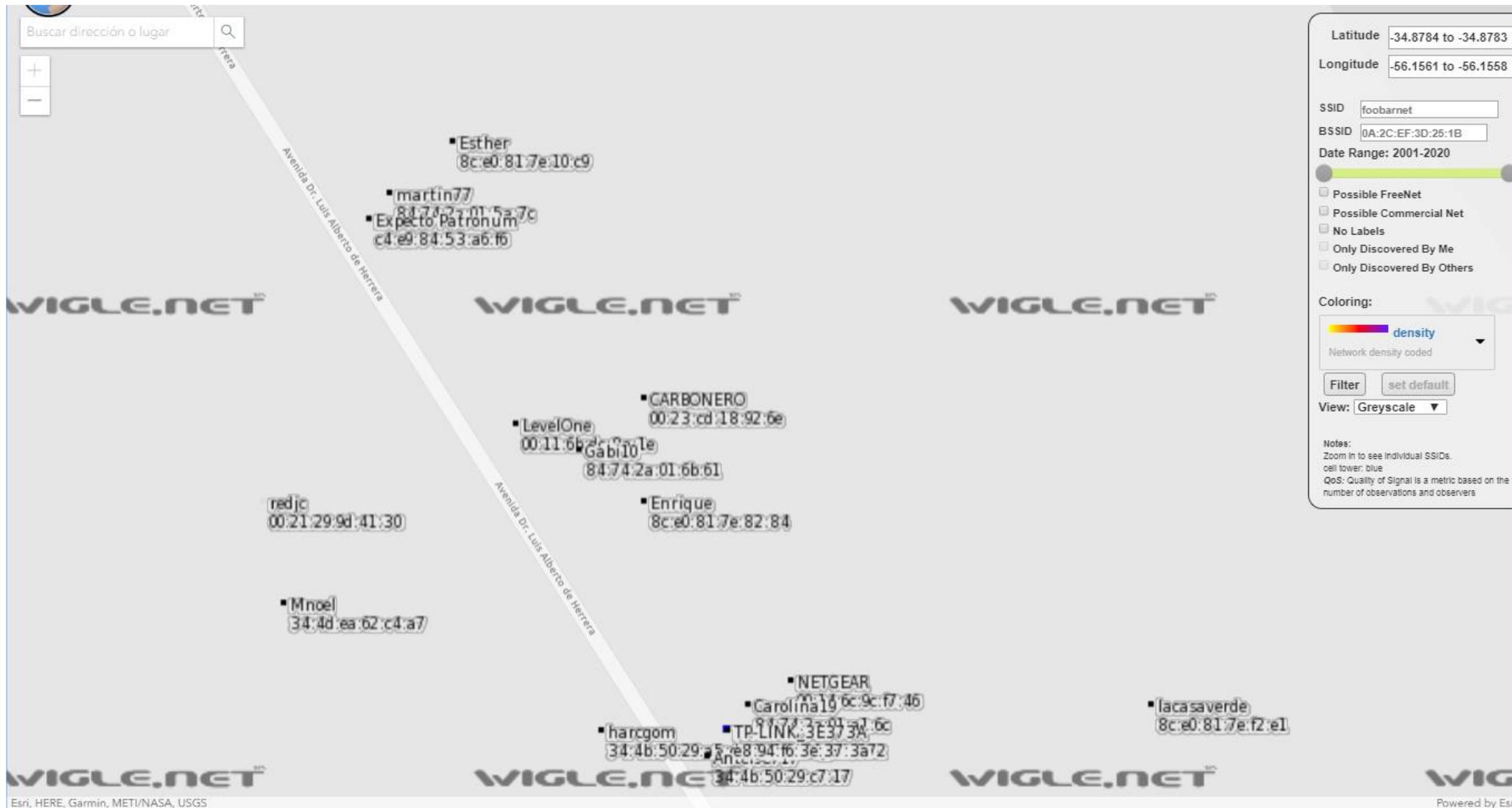




<http://wagle.net/>





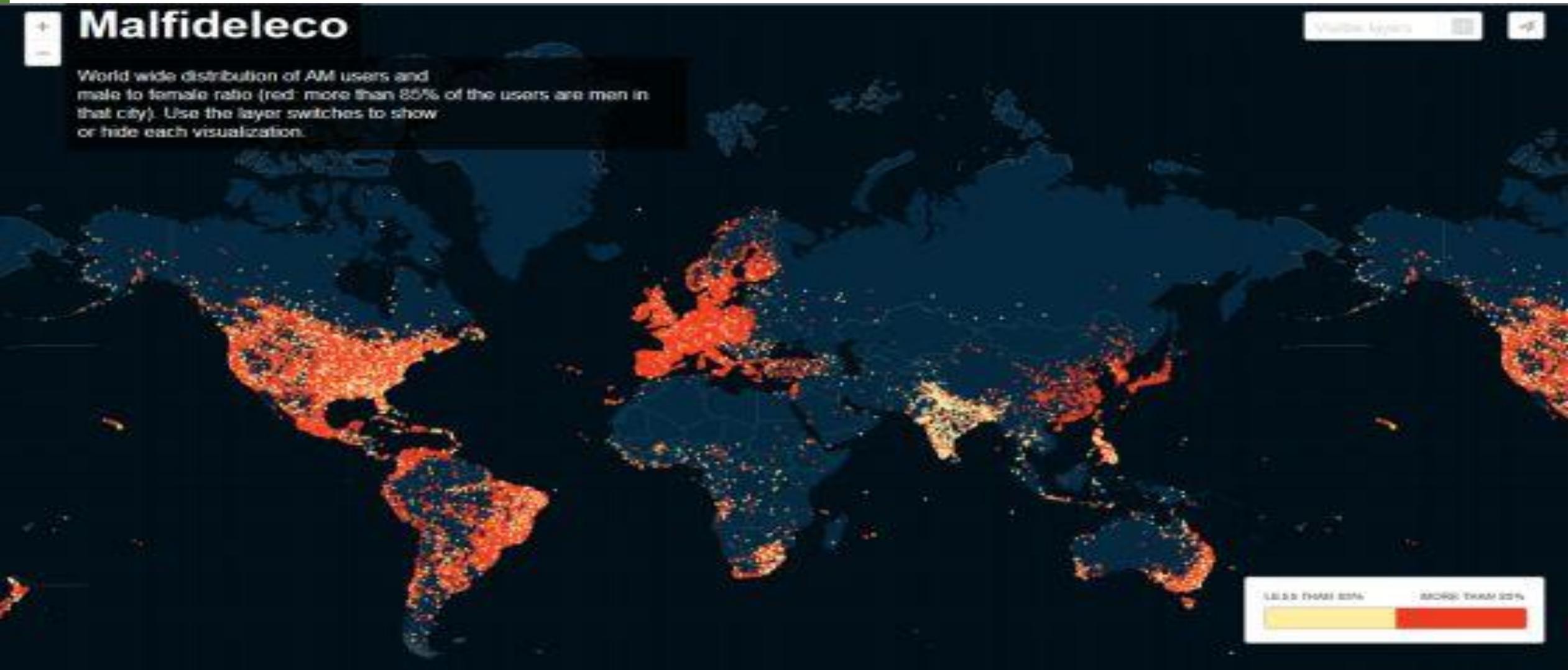




Malfideleco

World wide distribution of AM users and male to female ratio (red: more than 85% of the users are men in that city). Use the layer switches to show or hide each visualization.

Visible Layers  





Un mapa muestra dónde están los usuarios de Ashley Madison

Con los datos de Ashley Madison, crearon un mapa global que muestra dónde están los infieles. Filtrando la información del mapa por cantidad de usuarios, algunas ciudades uruguayas superan ampliamente el millar.

20.08.2015 09:33

 [Tuitear](#)

 [Me gusta 0](#)

[Compartir](#)

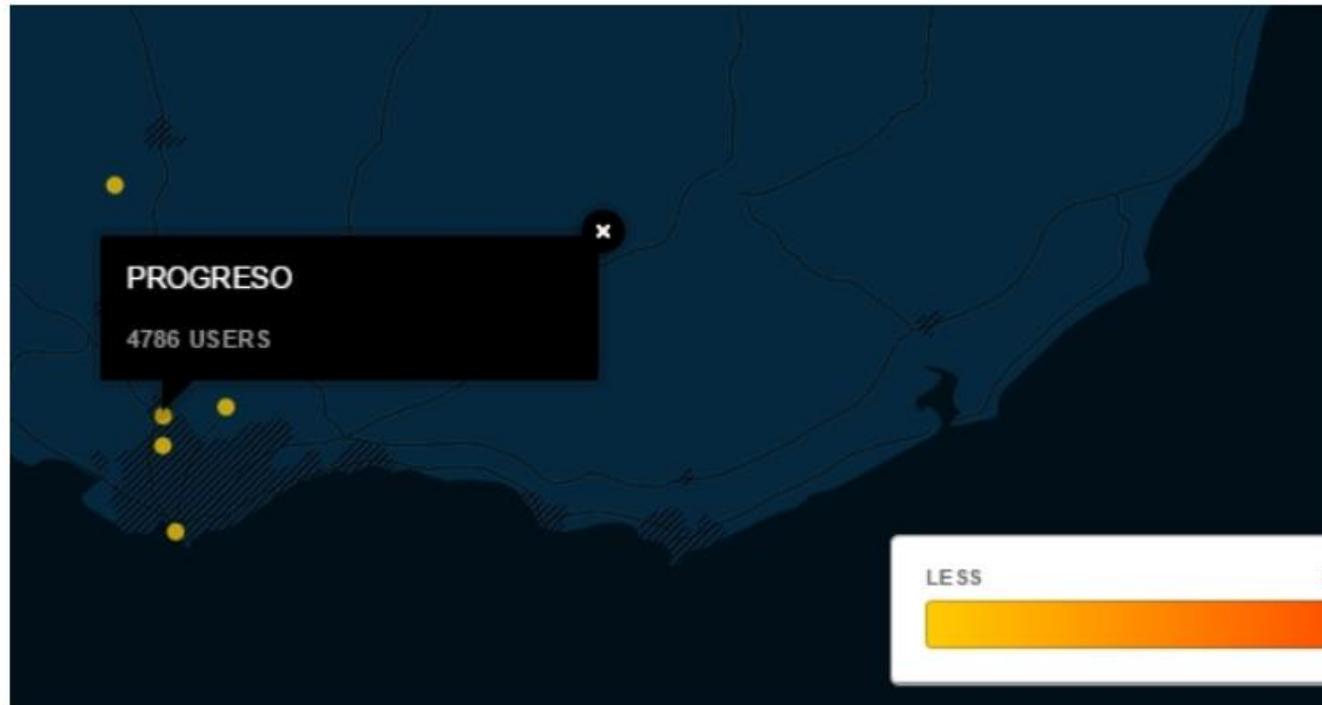
 [Compartir](#)



i.net...



Buscamos Uruguay y aparecieron pintadas de rojo, varias localidades. Filtramos por número de usuarios y aparece la ciudad de Progreso con 4.786 usuarios, seguida de Salto con 1.926. Sauce tiene 13 usuarios, y Montevideo 296.



Siempre que se detecta un usuario de una ciudad específica, se pinta el lugar. Si hay más de un 85 % de hombres, se pinta de rojo, en caso contrario, de amarillo.

'Hackeo' masivo a una popular web de citas: se filtran más de 400 millones de cuentas

Ha dejado la filtración de datos de Ashley Madison en pañales. Un ataque ha expuesto los datos de cientos de millones de usuarios, incluidos algunos que se habían dado de baja

The screenshot displays the Ashley Madison website interface. At the top, the logo "Ashley FriendFinder" is visible with the tagline "Relaciónate, encuentra sexo o conoce a alguien ahora". Navigation links include "¡Únete ahora!", "Página principal", "Navegar", "Encuentros", "Foros de citas", and "Chat en vivo". A login section at the top right contains fields for "Nombre de usuario" and "Contraseña", with a "Acceder" button and a link for "¿Olvidaste tu contraseña?".

The main content area features a large image of a woman with the text: "Únete a la comunidad de sexo e intercambio de parejas más grande del mundo". Below this, statistics are listed: "871 Transmisiones en Vivo | 98,897,765 Fotos sexis | 4,936,818 Conexiones".

On the right side, a registration form titled "¡Regístrate Ahora! ¡Empieza a ligar esta noche!" is shown. It includes a dropdown for "Soy/Somos:" (set to "Hombre"), checkboxes for "Interesado(s) en:" (Hombres, Mujeres, Parejas / Grupos, TS/TV/TG), a date picker for "MI fecha de nacimiento:", a "País:" dropdown (set to "España"), and a "Comunidad:" dropdown (set to "Cualquiera"). A "Regístrate ahora" button is at the bottom of the form.

MUNDO FACEBOOK MARK ZUCKERBERG ESTADOS UNIDOS CAMBRIDGE ANALYTICA

Facebook: Multimillonarias pérdidas para Mark Zuckerberg tras escándalo de filtración de datos

El escándalo de **Cambridge Analytica** ha pasado una fuerte factura a **Zuckerberg**, creador de **Facebook**, que ha visto sus acciones desplomarse.



20 Mar 2018 | 1



HACKING

Uber reconoce un robo de datos que afecta a más de 57 millones de usuarios



- La compañía pagó a dos hackers 100.000 dólares en 2016 para ocultar el ciberataque

EFE

22/11/2017 00:01

Actualizado a
22/11/2017 08:35



Oficinas centrales de Uber en San Francisco. Colorado (Eric Risberg / AP)

La plataforma de transporte compartido **Uber** desveló una **filtración** cibernética que la compañía había mantenido en secreto hasta hoy y que en **2016** afectó a los **datos personales de 57 millones de sus usuarios y conductores** en todo el mundo

IM firmó un acuerdo “confidencial” con el gigante chino Huawei para explorar proyectos de “ciudades inteligentes”

🕒 4 min ✓ 2 💬 1

Nº2020 - 16 AL 22 DE MAYO DE 2019

El concepto de smart cities o “ciudades inteligentes” resuena cada vez más en un mundo que se jacta de apuntar al desarrollo sostenible de las sociedades y al manejo eficaz de los recursos. Actualmente, muchas ciudades persiguen ese objetivo y buscan aplicar tecnologías de la información a áreas como el transporte, la recolección de residuos, el capital humano y la comunicación, de forma de mejorar la calidad de vida de los ciudadanos...

"Los esfuerzos por proteger el espacio digital no han avanzado al mismo ritmo que el proceso de digitalización"

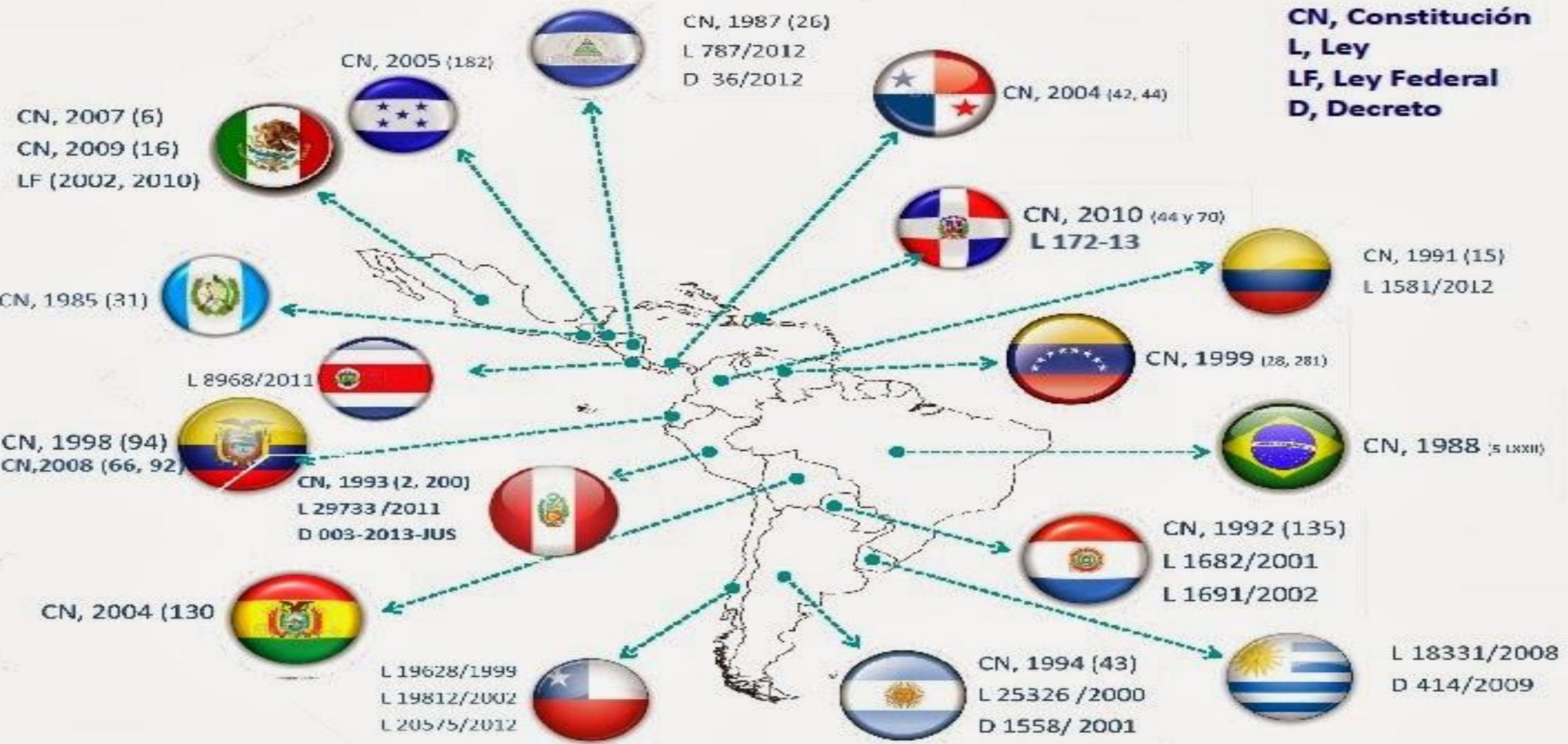
El gobierno contrata un préstamo del BID en ciberseguridad

🕒 4 min

№2017 - 25 DE ABRIL AL 01 DE MAYO DE 2019

Uruguy se transformó en uno de los países más desarrollados de la región en gobierno digital, comercio electrónico, así como en el uso de tecnologías de la información y la comunicación (TIC). Por ejemplo, el 95% de los trámites con oficinas gubernamentales pueden ser iniciados en línea; se expide la cédula de identidad con chip e información biométrica, y está implementándose la historia clínica electrónica. El costado negativo de esa fuerte penetración es el aumento de los riesgos potenciales...

CN, Constitución
L, Ley
LF, Ley Federal
D, Decreto



Mapa Latinoamericano sobre la protección de datos personales: Constituciones y normas generales (1985-2014/Feb)
 Nelson Remolina Angarita©, Universidad de los Andes, Bogotá, Colombia



Inicio- Legislación- Uruguay

Legislación



URUGUAY

Constitución

Artículo 7. - "Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad. (.....)."

Artículo 11. - "El hogar es un sagrado inviolable (...)."

Artículo 28. - "Los papeles de los particulares y su correspondencia epistolar, telegráfica o de cualquier otra especie, son inviolables."

Artículo 72.- La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno.

Artículo 332. - Los preceptos de la presente Constitución que reconocen derechos a los individuos, así como los que atribuyen facultades e imponen deberes a las autoridades públicas, no dejarán de aplicarse por falta de la reglamentación respectiva, sino que ésta será suplida, recurriendo a los fundamentos de leyes análogas, a los principios generales de derecho y a las doctrinas generalmente admitidas.

Legislación General

Ley N° 18.331, de 11 de noviembre de 2008. Protección de Datos Personales y Acción Habeas Data.

<http://www.redipd.es/legislacion/uruguay-ides-idphp.php> *

Legislación General

Ley N° 18.331, de 11 de noviembre de 2008. Protección de Datos Personales y Acción Habeas Data.

Ley N° 18.381, de 7 de noviembre de 2008. Acceso a la Información Pública.

Ley N° 18.719, de 27 de diciembre de 2010. Presupuesto Nacional para el ejercicio 2010-2014. Modifica los arts. 9, 14, 15, 16, 17, 21, 22, 28, 29, 34 y 35 de la Ley N° 18.331.

Ley N° 18.812, de 7 de septiembre de 2011. Información de la Central de Riesgos Crediticios del Banco Central de Uruguay. Establece el marco jurídico para garantizar el acceso a la información contenida en dicha Central de Riesgos.

Ley N° 18.996, de 7 de noviembre de 2012. Rendición de cuentas y balance de ejecución presupuestal del ejercicio 2011. A través de su artículo 43, incorpora modificaciones a la Ley N° 18.331 en lo que se refiere a la definición de lo que se consideran fuentes públicas o accesibles al público.

Ley N° 19.030, de 7 de enero de 2013. Aprobación del Convenio 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y su Protocolo Adicional.

Decreto N° 664/008, de 22 de diciembre de 2008. Crea el Registro de Bases de Datos Personales, adscrito la URCDP.

Decreto N° 414/2009, de 31 de agosto de 2009. Reglamento de desarrollo de la Ley N° 18.331. Adecuación a la Directiva 95/46/CE.

Legislación Sectorial

Ley N° 15.322, de 17 de septiembre de 1982. Ley de intermediación financiera. Artículo 25 (secreto bancario).

Ley N° 16.099, de 13 de noviembre de 1989. Ley de Prensa: regula la libertad de comunicación de pensamientos e información, y consagra el derecho de respuesta.

Ley N° 17.823, de 7 de septiembre de 2004. Código de la Niñez y la Adolescencia.

Ley N° 17.835, de 23 de septiembre de 2004. Limitante relativa a la normativa sobre secreto.

Ley N° 18.244, de 27 de diciembre de 2007. Se establecen normas para el tratamiento de datos de los deudores alimentarios

*** Impresión ilustrativa de la web redidp, han habido cambios normativos que no figuran en dicho sitio**

ESTÁNDARES DE PROTECCIÓN

DE DATOS PERSONALES

RED
IBEROAMERICANA DE
PROTECCION
DE DATOS





DEPARTAMENTO DE DERECHO INTERNACIONAL (DDI)

OEA » SAJ » Departamento de Derecho Internacional (DDI) » Protección de Datos Personales » Ley Modelo Interamericana

Protección de Datos Personales

Desarrollos normativos por país

Documentos de Referencia

Jurisprudencia

Ley Modelo Interamericana

Documentos de Referencia

Ley Modelo Interamericana sobre Protección de Datos Personales (en elaboración)

En esta sección podrá encontrar los documentos que han formado y formarán parte del proceso de preparación, discusión y aprobación de la Ley Modelo Interamericana sobre Protección de Datos Personales.

Introducción

En esencia, una ley modelo establece parámetros generales, una hoja de ruta, que puede ser incorporada completa o parcialmente en la legislación interna de un Estado, sirviendo

Documentos Relacionados

- [Ley Modelo Interamericana sobre Acceso a la Información](#) [En](#) | [Fr](#) | [Pt](#)
- [Guía de Implementación de la Ley Modelo](#) [En](#) |

Sitios Relacionados

[Documentos OEA](#)

[Desarrollos en otras](#)

Asia-Pacific
Economic Cooperation

APEC Cross-Border Privacy Rules (CBPR) System



In November 2011, the APEC Leaders issued a directive to implement the [APEC Cross Border Privacy Rules \(CBPR\)](#) system. The CBPR system balances the flow of information and data across borders while at the same time providing effective protection for personal information, essential to trust and confidence in the online marketplace. The system is one by which the privacy policies and practices of companies operating in the APEC region are assessed and certified by a third-party verifier (known as an accountability agent) and follows a set of commonly agreed upon rules,

based on the [APEC Privacy Framework](#). By applying this commonly agreed-upon baseline set of rules, the CBPR system bridges across domestic differences that may exist among domestic privacy approaches. Currently, six APEC member economies—Canada, Japan, Republic of Korea, Mexico, Singapore and the United States—have aligned their privacy laws with the APEC Privacy Framework.

APEC Privacy Recognition for Processors (PRP) System

The [Privacy Recognition for Processors System \(PRP\)](#) governance documents were endorsed by APEC in August 2015. The PRP system is designed to help personal information processors assist controllers in complying with relevant privacy obligations, and helps controllers identify qualified and accountable processors. This is done through an [intake questionnaire](#), which sets forth the baseline requirements of the PRP. The APEC-recognized accountability agent will then assess a processor seeking recognition based on a set of requirements. Currently, two APEC member economies—Singapore and the United States—have joined the PRP System.

APEC Privacy Framework

The [updated APEC Privacy Framework 2015](#) addresses the gaps in policies and regulatory frameworks on e-commerce to ensure that the free flow of information and data across borders is balanced with the effective protection of personal information essential to trust and confidence in the online market place. The update of the Privacy Framework was endorsed by ministers in November 2016.

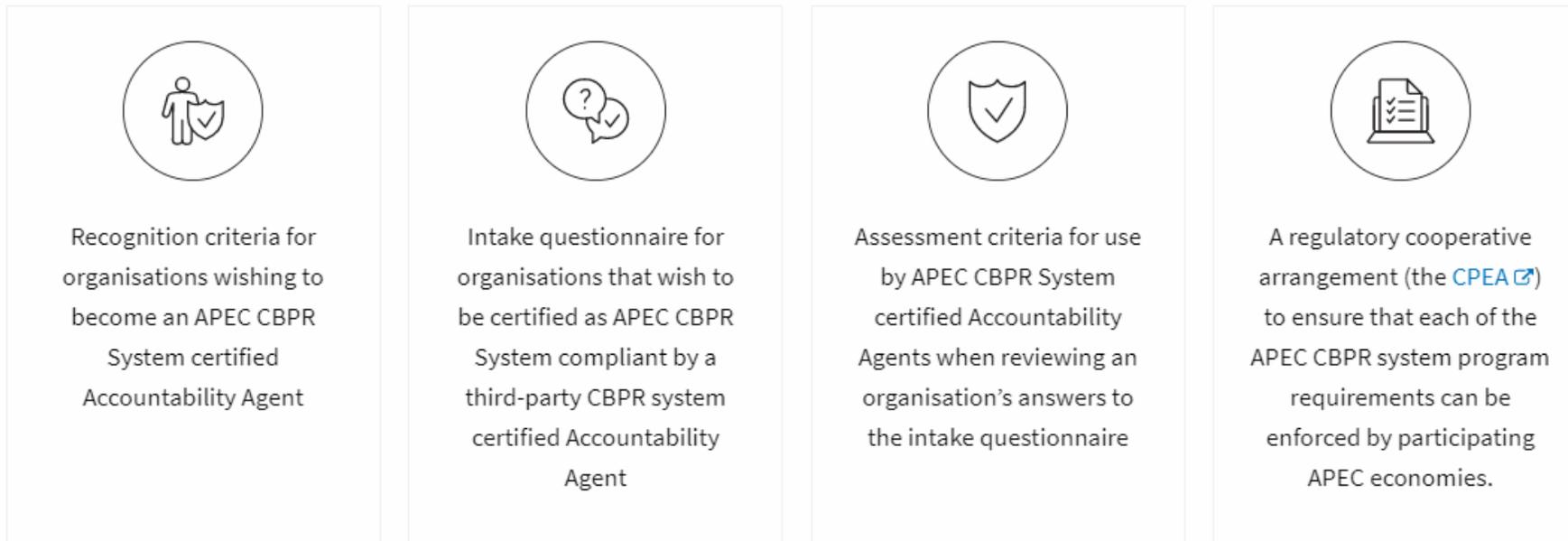
Promoting Interoperability between the APEC – EU Privacy Rules Systems





The APEC Cross-Border Privacy Rules (CBPR) System, endorsed by APEC Leaders in 2011, is a voluntary, accountability-based system that facilitates privacy-respecting data flows among APEC economies.

It has four main components:



La Comisión y sus prioridades

Políticas, información y servicios



español 

Buscar

Inicio > Legislación > Legislación por temas > Protección de datos

Protección de datos

Normas sobre protección de datos personales dentro y fuera de la UE.

La protección de datos en la UE

El Reglamento general de protección de datos (RGPD), la Directiva sobre la policía y otras normas sobre protección de datos personales y las autoridades encargadas de aplicarlas.

International dimension of data protection

Rules on international data transfers
Adequacy decisions
EU-US data transfers
Standard Contractual Clauses (SCC)
Binding Corporate Rules (BCR)
Transfer of air passenger name record data and terrorist finance tracking programme

Reform

Derechos de los ciudadanos
Normas para empresas y organizaciones
¿Qué son los datos personales?
¿Qué rige el Reglamento general de protección de datos («RGPD»)?
¿Qué constituye tratamiento de datos?
¿Qué son las autoridades de protección de datos (APD)?

Protección de Datos Personales

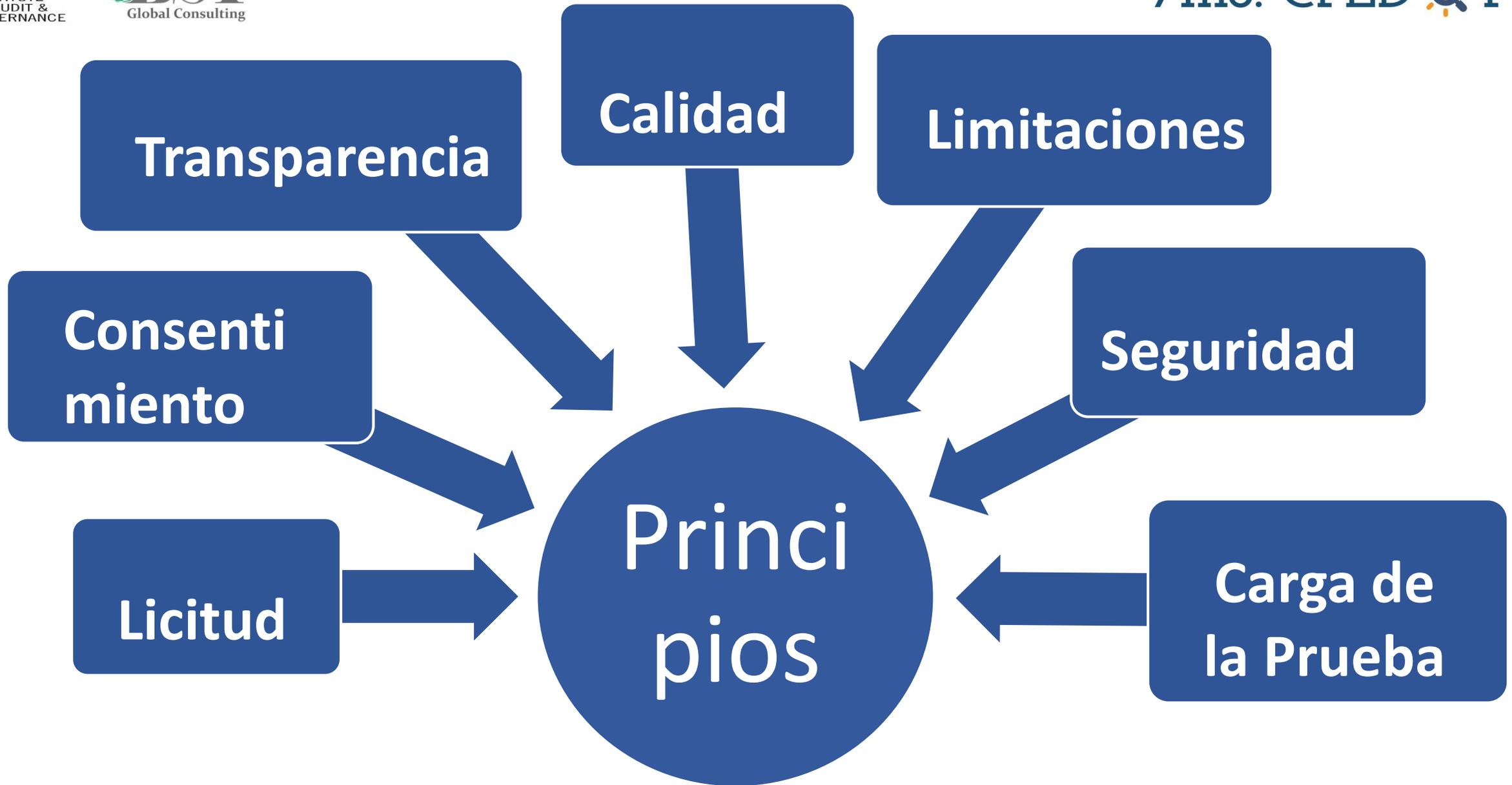
4.5.2016 ES Diario Oficial de la Unión Europea L

I
(Actos legislativos)

REGLAMENTOS

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO
de 27 de abril de 2016
relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales
y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento
general de protección de datos)

(Texto pertinente a efectos del EEE)



OBTENER

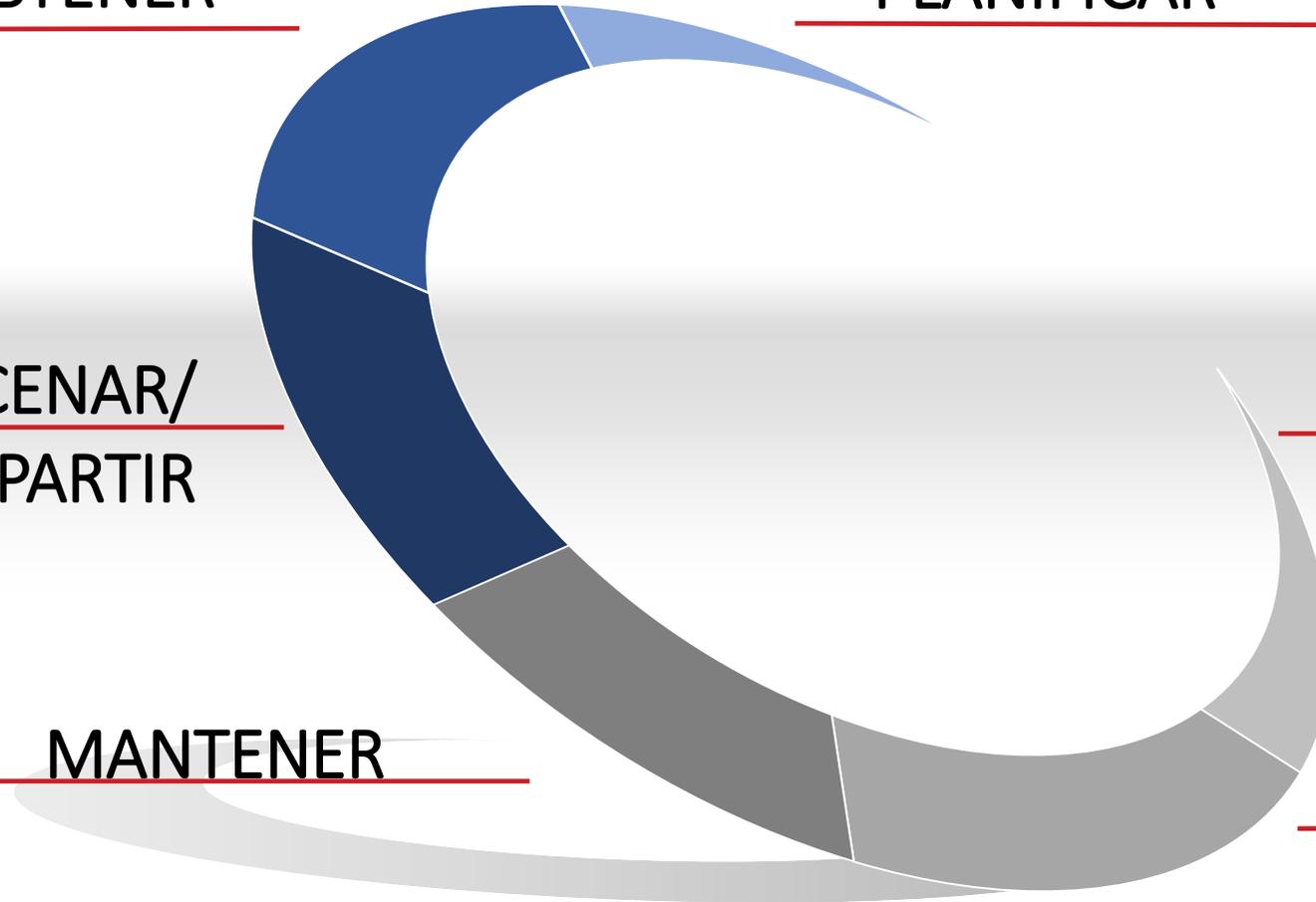
PLANIFICAR

ALMACENAR/
COMPARTIR

ELIMINAR

MANTENER

PROCESAR



¿Qué datos
personales
necesitamos?

¿Por qué los
necesitamos?

¿Para qué los
usaremos?

¿Con quién los
compartiremos?

¿Por qué los
compartiremos?

¿Por qué
necesitamos datos
personales
sensibles?

¿Cómo los
obtendremos?

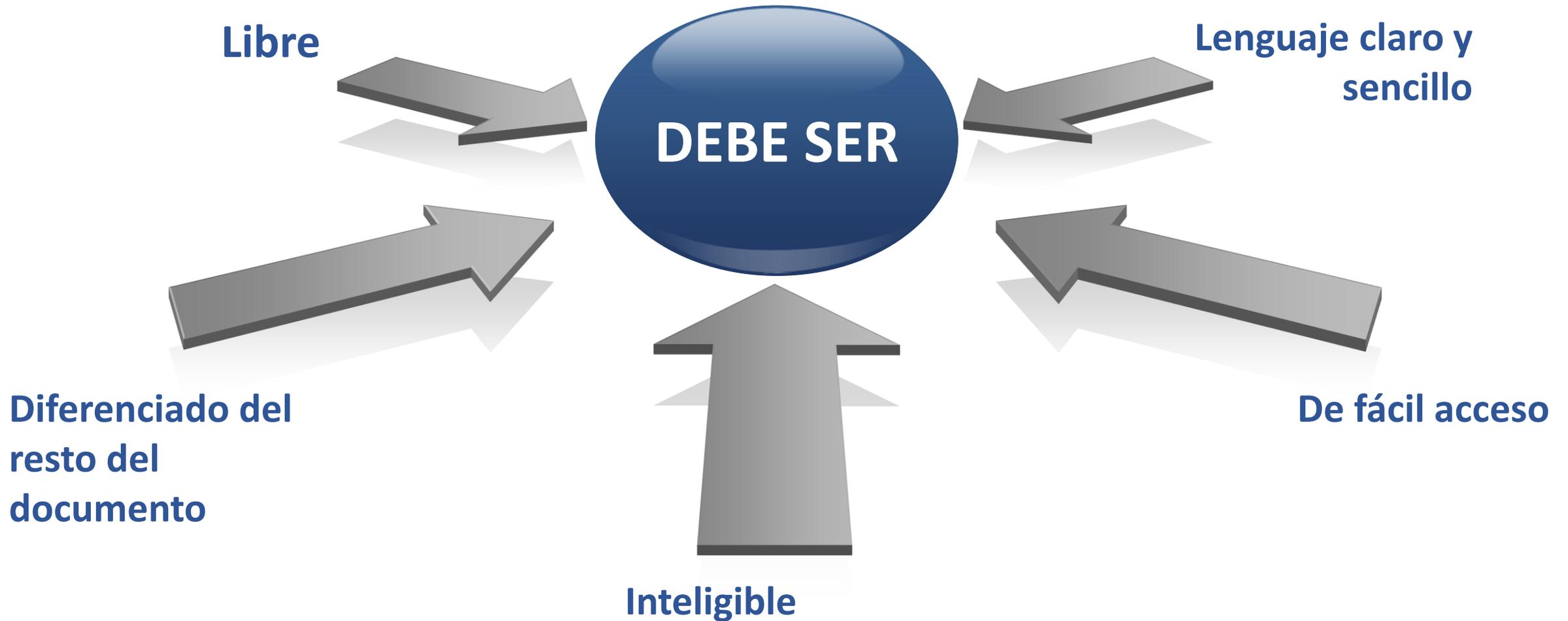
¿Cómo nos
comunicaremos con el
titular?

¿Cuáles son los
procedimientos que
emplearemos para
obtener estos datos
personales?

¿Obtendremos datos
personales precisos con
estos procedimientos?

¿Cómo aseguraremos la
calidad?

Consentimiento



*No será vinculante ninguna parte de la declaración que constituya infracción al GDPR

¿Cómo y Dónde serán almacenados?

¿Podremos encontrarlos de nuevo fácilmente?

¿Los estamos almacenando simultáneamente en otros lugares?

¿Cómo aseguraremos la integridad de los datos personales?

¿Podemos transferirlos?
(Consentimiento, BCR, Lista)

¿Es segura la transferencia?

¿Los datos transferidos serán procesados de acuerdo al GDPR?

¿Estamos actualizando los datos personales?

¿Cómo corregimos los errores?

¿Podemos corregir todas las copias al mismo tiempo?

¿Estamos actualizando el consentimiento?

¿Podemos actualizar el consentimiento para otros fines?

«La reglamentación determinará las medidas que correspondan según los tipos de datos, tratamientos y responsables, así como la oportunidad para su revisión y actualización.» Art. 12 in fine LPDDPP en la redacción dada ley 19.670 (En.2019)

MEDIDAS DE SEGURIDAD

Medidas de
Seguridad Jurídicas

Medidas de
Seguridad
Organizativas

Medidas de
Seguridad Técnicas



¿Estamos procesando los datos personales de acuerdo a cómo lo planificamos?

Estamos procesando los datos en que el consentimiento ha cambiado de la misma forma?

¿Podemos atender todos los derechos?

¿Los procedimientos mantienen los datos personales seguros?

¿Podemos probar que todo el procedimiento está acorde con el GDPR?



¿Necesitamos
mantener esta
información?

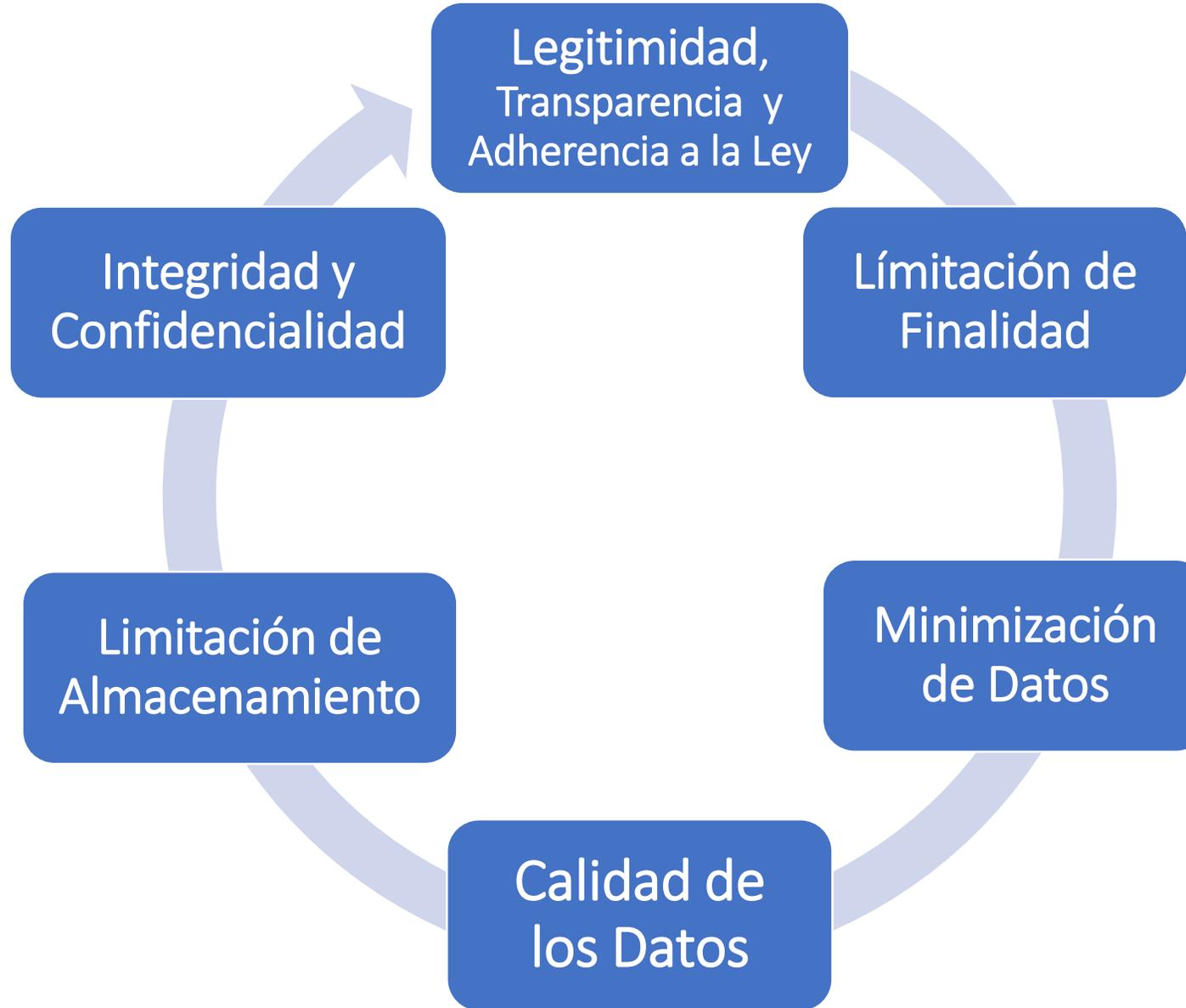
¿Hemos informado
acerca de ello?

¿Cómo nos
deshacemos de los
datos personales?

¿Es segura nuestra
forma de eliminar
datos?

¿Podemos
deshacernos de
todas las copias al
mismo tiempo?

BENEFICIOS



Principios LPDDPP

- Legalidad.
- Veracidad.
- Finalidad.
- Previo consentimiento informado.
- Seguridad de los datos.
- Reserva.
- Responsabilidad.

Últimas noticias

EDPB NEWS NATIONAL NEWS

Programa

PROGRAMA COMPLETO



EDPB Tenth Plenary Press Release

15 May 2019



EDPB Tenth Plenary Session of the European Data...

14 May 2019



EDPB Comité Europeo de Protección de Datos – 9.º Sesión Plenaria

10 April 2019



EDPB Ninth Plenary Session

09 April 2019

EU Open Days 2019

04 May 2019

Tenth Plenary Session of the EDPB - 14 & 15 May 2019

14 May 2019

Eleventh Plenary Session of the EDPB - 4 & 5 June 2019

04 June 2019

Twelfth Plenary Session of the EDPB - 9 & 10 July 2019

09 July 2019



European Data Protection Board



Particulares

- > Directrices sobre sus derechos
- > Póngase en contacto con la autoridad de protección de datos apropiada



Responsables y encargados de tratamiento

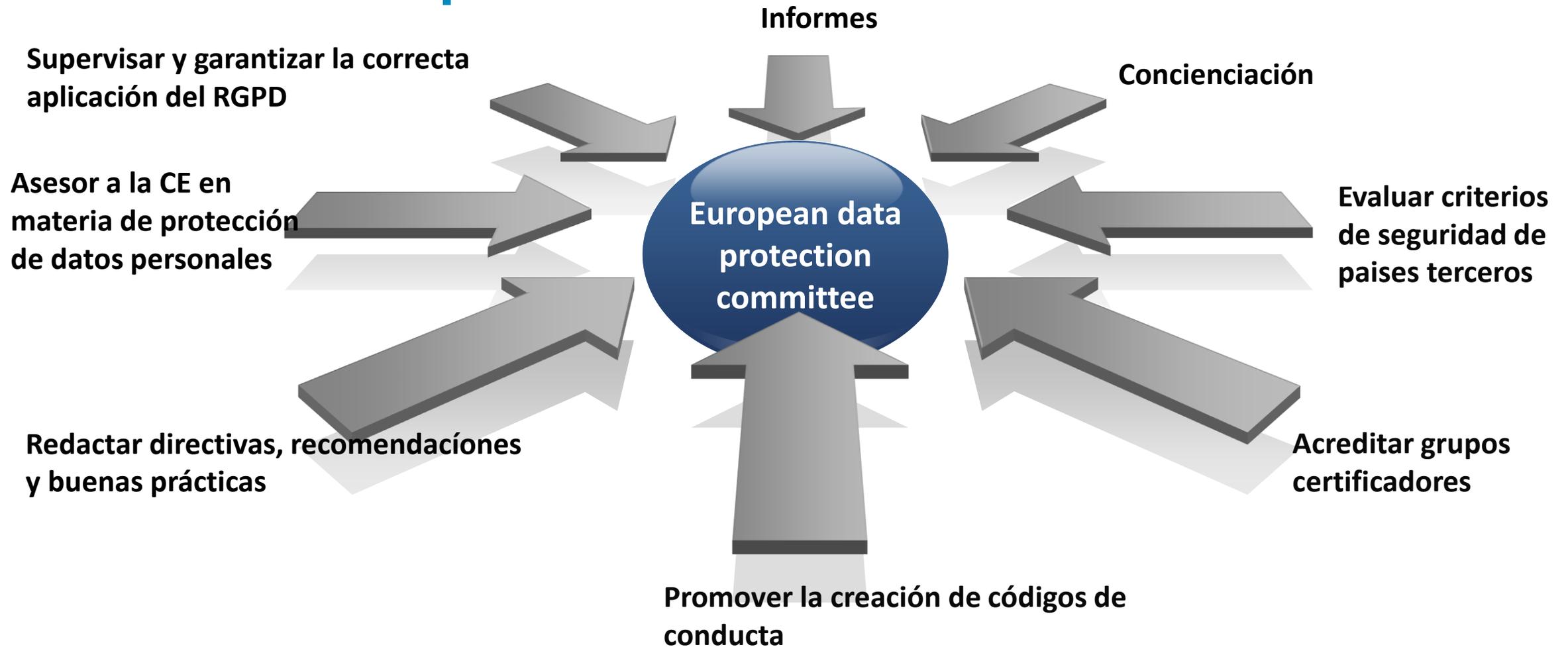
- > Directrices para los Responsables y encargados de tratamiento
- > Póngase en contacto con la autoridad de protección de datos apropiada



Reguladores

- > Función del CEPD
- > Opiniones del CEPD relativas a propuestas legislativas

European Data Protection Board



¿Hay «Compliance» más allá del PLDFT?

- **Riesgo de Cumplimiento:** *Riesgo Sanciones Normativas, Pérdida financiera material, Pérdida de reputación - Incumplir – Leyes, Regulaciones, Normas, Estándares - Códigos de conducta*
- **Normas de Cumplimiento:** *Conducta del Mercado; Conflictos de Interés; Trato justo a clientes; Idoneidad del Asesoramiento; PLFT; Leyes tributarias...*

COMITÉ DE BASILEA DE SUPERVISIÓN BANCARIA - EL CUMPLIMIENTO Y LA FUNCIÓN DE CUMPLIMIENTO EN LOS BANCOS - ABRIL, 2005



Función de Cumplimiento vs Oficial de Cumplimiento

***Función de Cumplimiento** = Personal a cargo de Responsabilidades de Cumplimiento*

***El Encargado o Jefe de Cumplimiento** = Responsabilidad general de coordinar la identificación y administración del riesgo de cumplimiento y supervisar las actividades del personal de cumplimiento*

*A veces jefe de cumplimiento = **“oficial de cumplimiento”***

*Otras veces **“oficial de cumplimiento”** = Persona que ejecuta responsabilidades específicas dentro cumplimiento.*

Función de Cumplimiento vs Oficial de Cumplimiento



dreamstime

- **Riesgo de cumplimiento** = Posibilidad afectada por violar Leyes, Regulaciones, Estándares Prácticas o Estándares Éticos.
- **Función de cumplimiento** = Responsable del seguimiento del cumplimiento de Legislación, Gobierno Corporativo, Regulaciones, Códigos Políticas
- **Oficial de Cumplimiento** = responsable de la implantación, seguimiento y control del sistema de prevención de LA/FT.

La Seguridad de la Información – Función de Cumplimiento



Fuente: dreamstime

La institución debe realizar una gestión integral e independiente de la Seg Inf

Estándares, Procedimientos preservar la confidencialidad, integridad y disponibilidad de la información, teniendo en cuenta seguridad física y lógica.

Identificar, evaluar, tratar y monitorear los riesgos asociados a la gestión de sus activos de información, analizar las amenazas y vulnerabilidades.

Monitoreo de la gestión de la Seg Inf

Capacitación al personal en la gestión de los riesgos asociados.

Asegurar el cumplimiento de las políticas de seguridad de la información de las actividades tercerizadas, y velar por la seguridad de los datos procesados externamente. (...))»



Fuente: www.eldefinido.cl

Marco Normativo General Uruguayo

- *Ley 18.331 (Ag.2008) y concordantes.- Protección DDPP*
- *Dec.414/019 (Ag. 2009) y concordantes.- Reglamentario de la ley 18.331*
- *Ley 18.381 (Nov.2008) y concordantes.- Acceso a la información pública*
- *Dec.232/010 (Ag. 2010) y concordantes.- Reglamentario de la ley 18.381*

Recientes modificaciones al marco normativo nacional

• Ley 19.670 «RC 2017» Oct.2018 (vigor 2019)

- Art. 37.- Modifica el ámbito de aplicación de la ley PDDPP (aplicación extraterritorial);
- Art. 38.- Deber de informar las vulneraciones de seguridad al titular y a la URCDPP;
- Art. 39.- Reformula el principio de responsabilidad consagrando el criterio de «Responsabilidad Proactiva» (Art. 12 ley PDDPP).
- Art. 40.- Obligación de designar un «Delegado de Protección de Datos» para entidades públicas y determinadas empresas privadas.

gub.uy

Ingresá a

Unidad Reguladora y de Control de Datos Personales
URCDP

¿En qué podemos ayudarte? URCD

Institucional Políticas y Gestión Trámites y Servicios Datos y Estadísticas Comunicación

Inicio > Publicaciones > Cambios recientes a legislación sobre Protección de Datos Personales en Uruguay

Informes

Cambios recientes a legislación sobre Protección de Datos Personales en Uruguay

25 de Enero, 2019

En enero de 2019 entró en vigencia la nueva Ley de Rendición de Cuentas, que incorpora importantes modificaciones a la legislación nacional sobre Protección de Datos Personales con el fin de ofrecer mayores garantías a los uruguayos.

- La Ley 18.331 amplía su ámbito de aplicación fuera del territorio de Uruguay.
- Las entidades públicas y privadas deben incorporar la figura del delegado de protección de datos.
- Los responsables y encargados de las bases de datos están obligados a informar las vulneraciones de seguridad.
- Los responsables y encargados de las bases de datos deben velar por el cumplimiento y protección de las disposiciones de la ley.

Tienes permiso para meterte en su vida?
Le explicaste lo que puede pasar si te
miente? Le diste la oportunidad de
corregirte? Le diste la opción de borrar
todos sus datos? Les pediste permiso para
verificar los datos?

Quién es? A qué se
dedica? Cuánto gana?
Cómo generó la \$\$?
Qué pretende hacer
con esa \$\$? Está
casado? Dónde vive?
Has documentado?

Tratamiento de DDPP y «Compliance»

- **Existe la excepción de responsabilidad para la realización del ROS y para las facultades inspectivas PERO ¿el Tratamiento de los DDPP y los derechos del titular frente al tratamiento?**

Tratamiento de DDPP y «Compliance»

Obligación de tratar datos personales

Exención del consentimiento previo informado:

9.A Fuentes públicas o medios masivos de comunicación.

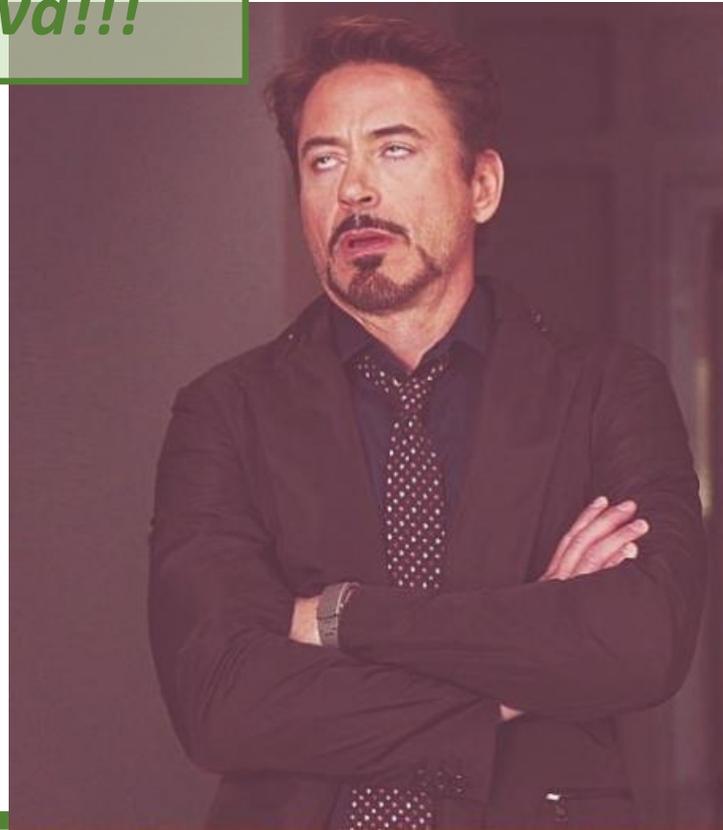
9.B En virtud de una obligación legal.

9.C Datos limitados (nombres y apellidos, documento de identidad, nacionalidad, domicilio, fecha de nacimiento; razón social, nombre de fantasía, registro único de contribuyentes, domicilio, teléfono e identidad de las personas a cargo de la misma).

9.C Relación contractual, científica o profesional del titular de los datos, y sean necesarios para su desarrollo o cumplimiento.

De «*Lege Ferenda*» - Tratamiento de DDPP y «Compliance» - Ejemplo Español

-Tengo derecho de autodeterminación informativa!!!



Art. 32 Ley 10/2010 Española.- Con fines de PLDFT: No se requiere consentimiento previo para el tratamiento de DDPP; no existe obligación de información; no rigen derechos de acceso rectificación, cancelación y oposición respecto a los ficheros . Se deben aplicar medidas de seguridad de alto nivel

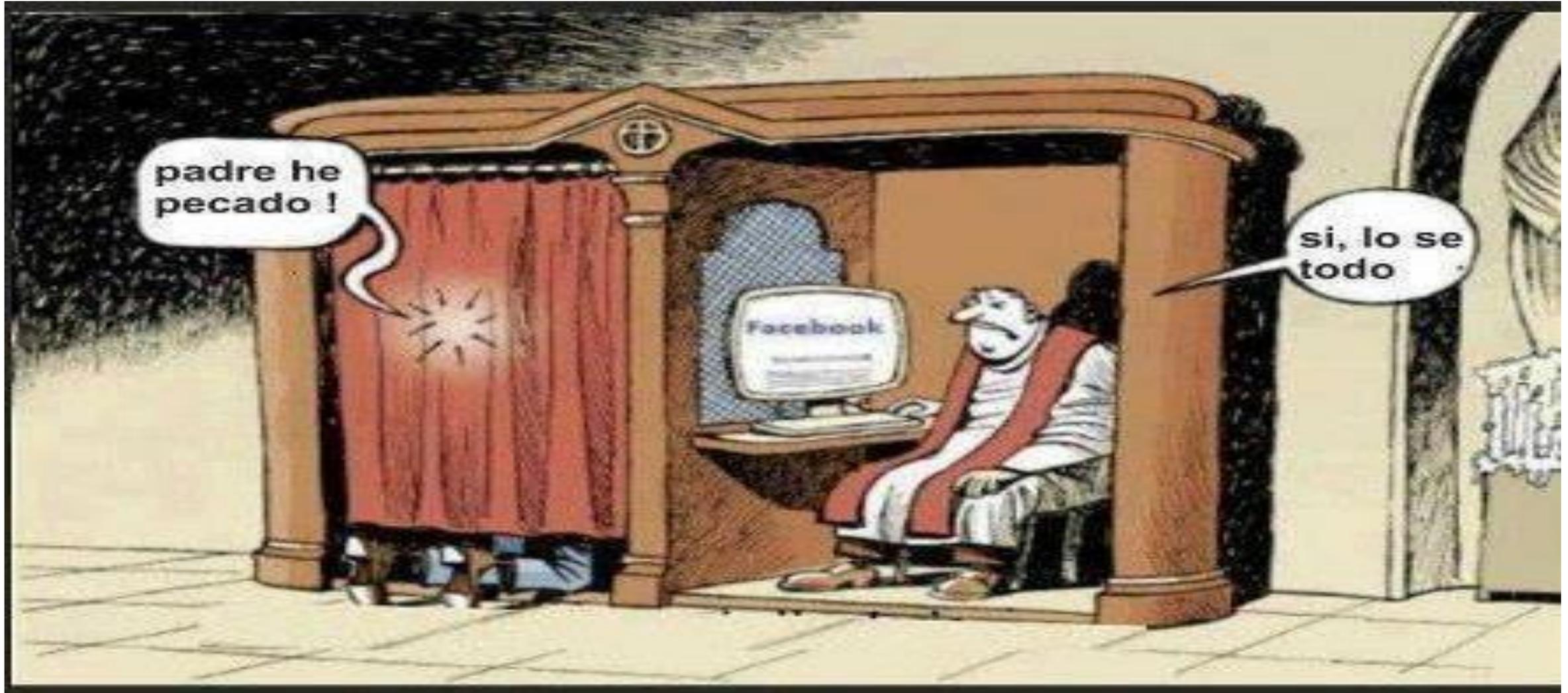
De «*Lege Ferenda II*» - Comunicaciones de DDPP y «Compliance» - Ejemplo Español



Art. 33 Ley Española: Se permite la comunicación entre SO con la sola finalidad de prevenir o impedir actos de LAFT cuando se concluya que una persona puede intentar repetir una operación que le haya sido rechazada. Se permite expresamente la consulta de fichero creados con la finalidad de PLDFT por el personal de control interno de los SO



Es mejor pedir permiso que pedir perdón



Muchas gracias

Antoni Bosch Pujol,
CISA, CISM, CGEIT, ECPD

Director General Institute of Audit & IT-Governance.

www.iaitg.eu

Director Máster en Auditoría, Seguridad, Gobierno y Derecho de las TIC de la Universidad Autónoma de Madrid.

www.uam.es/masgdtic

Profesor de la Pacífico Business School

antoni.bosch@iaitg.eu

Francisco Olaso Martins
Abogado, CAMS, CAI

Consultor en BST Global Consulting

www.bst.consulting

Docente en Certificado de Prevención de Lavado de Dinero y Financiamiento del Terrorismo; UCU Business School

<https://ucubs.edu.uy/programas-focalizados/prevencion-lavado-dinero>

folaso@bst.consulting